IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 3:18-cr-00074-JAG
	)	
JOHN GLENN WEED,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

The United States of America, by and through its attorneys, G. Zachary Terwilliger, United States Attorney for the Eastern District of Virginia, and Brian R. Hood, Assistant United States Attorney, hereby responds in opposition to the defendant's Motion to Suppress. (Docket No. 17.) For the reasons set forth below, the defendant's motion and request for an evidentiary hearing should be denied.

I. INTRODUCTION AND FACTUAL SUMMARY

As set forth in a search warrant affidavit related to this case[1], the defendant, JOHN GLENN WEED, was a computer systems architect employed by The Analytic Sciences Corporation (TASC), Chantilly, Virginia, which was a contractor for the National Reconnaissance Office (NRO). While at TASC the defendant developed the Tactical Dissemination Network (TDN), which was a network designed to process and transmit information used by the military and the intelligence community in support of the United States' war against terrorism. As part of his duties, WEED also worked with radio transmitters commonly referred to as "Blue Force Trackers" ("BFTs") or "Friendly Force Trackers" ("FFTs"). These devices permit operational commanders to track the location of military and

[1] Case number 3:13-ms-235, filed August 23, 2013.

intelligence community assets, such as personnel and vehicles, while those assets conduct missions in operational theaters.

WEED was widely regarded by both peers and colleagues as a brilliant computer coder, but also had a widespread reputation for being a difficult employee and someone who behaved as if the rules did not apply to him. Prior to his termination, he was counseled on multiple occasions for security violations.

As part of a periodic reinvestigation (PR) for WEED's security clearance, an adjudications investigator learned that WEED had been arrested for Driving Under the Influence (DUI) in May 2012, which constituted the third known DUI arrest or conviction the defendant had received while working for TASC and the NRO.[2] The defendant did not report that arrest as required to government officials. The background investigator contacted WEED and scheduled an interview regarding the unreported DUI for September 18, 2012. On that day, the defendant contacted the investigator and stated that he would be unable to come in because he was working on "Iran issues." A review of public records revealed that one week before the proposed interview, on September 11, 2012, WEED had pleaded guilty in Fauquier County Circuit Court for a DWI violation, and that on September 18, 2012, the defendant made an appearance in Fauquier General District Court, which investigators believe was a probation violation hearing that flowed from the defendant's September 11 guilty plea.

The background investigator eventually interviewed WEED about the unreported DUI on September 20, 2012. WEED brought to the interview a photograph of the officer who arrested him for the DUI. The photo WEED displayed bore multiple bullet holes. The defendant stated that he got the picture off the Internet and used the picture of the arresting officer for "target

[2] The defendant's other DUI/DWI arrests and convictions occurred in the United Kingdom in 2005, which the defendant self-reported, and in Fauquier County, Virginia, on January 30, 2012.

practice." WEED believed he was unjustly convicted and that he intended to "ruin the life" of the arresting officer for what he did. WEED's conduct on this day quickly resulted in his being removed from the premises and barred from entering any TASC or NRO property and facilities. The defendant's security clearance was revoked and his employment officially terminated several weeks later.

Prior to his termination, WEED had been directed on numerous occasions by his superiors to provide all of the source code and information related to the design and function of the TDN. Even though the TDN was government property to which WEED had no ownership rights, WEED evidently resisted providing the requested information by repeatedly stalling or making excuses for not delivering his work product. WEED eventually turned over information related to the TDN when a supervisor told him that he would not be allowed to travel for his job until he had turned over information related to the TDN. This behavior, coupled with several statements by WEED that emerged during a post-termination review of his emails, suggested to investigators that WEED held an inappropriate attitude of individual ownership regarding his government work product.

Particularly concerning to NRO officials was information received from one of WEED's coworkers, who reported that WEED once stated words to the effect that "if they ever try to get rid of me I could plant back doors to gain remote access to bring down the system." Unsurprisingly, officials at TASC and NRO were not confident that they knew everything they should or needed to know regarding WEED's work on the TDN. These concerns prompted a security review of WEED's computer following his termination.

A forensic investigation of WEED's computer at the NRO revealed that on four consecutive days from September 17 to September 20, 2012, a remote desktop protocol (RDP)

session had been established from the defendant's workstation in the NRO to an external computer with the IP address of 71.61.115.229. Remote desktop protocol is a proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection. The defendant's workstation was located in an area called a sensitive compartmented information facility ("SCIF"), which is a secure area designed to safely store highly classified information. For security reasons, SCIFs typically are not designed to provide network access to the external Internet. NRO officials considered these RDP sessions highly suspicious because such connections to the external Internet from the SCIF were not authorized by the NRO's security policies and procedures, and moreover during the sessions there was an exchange of over 800 MB data that, because the data was both compressed and encrypted, investigators were unable to determine its contents.

Forensic analysis also revealed that the external computer that connected to WEED's NRO workstation was named "SUNBLOCK-FITPC2." WEED regularly used the nickname "Sunblock" in the signature line of his NRO emails because he considered himself so critical to the NRO's mission that he was a "single point of failure," also referred to as an "SPF," which is the same abbreviation for the "sun protection factor" used to rate the effectiveness of various suntan and sunblock lotions. A public records check revealed that IP address 71.61.115.229 was owned by Comcast, and records obtained from Comcast indicated that on the relevant dates above that IP address was assigned to the residential internet account for WEED's residence.

Based in part on the above information, FBI Special Agent Steve Hall obtained a search warrant for the defendant's residence in Fredericksburg, Virginia, on August 23, 2013, which agents executed on August 27, 2013. During the search, which investigators conducted 11 months after WEED was escorted from NRO facilities, investigators seized numerous items of

United States government property. Agents found one General Dynamics, Model AATR radio in a cardboard box in the defendant's garage. They also found 11 BFT transmitters stored in hard-shelled pelican cases lying in plain view on the floor in the defendant's basement workshop. These are identified in the pending indictment as "two (2) General Dynamics MTX, Version 1.4 transmitters; eight (8) General Dynamics, Trident Version 1.0 transmitters; [and] one (1) Model PGITR transmitter."

Numerous interviews with WEED's coworkers and supervisors at both TASC and the NRO failed to identify anyone who gave WEED permission to take these devices home and keep them as his personal property. These same interviews failed to identify anyone who knew that WEED had taken these devices home, and further did not suggest that either TASC or the NRO had a permissive work culture where people turned a blind eye to others taking home and permanently keeping government property. WEED also signed numerous nondisclosure agreements as part of his employment, all of which contained the provision that all property he obtained during his employment with TASC and the NRO remained government property and was to be returned to the government upon the termination of his employment. These 12 radios, the AATR and the 11 BFTs, thus became the basis for Count One of the defendant's indictment, charging him with theft of government property, in violation of Title 18, United States Code, Section 641.

II. ARGUMENT

In his motion, WEED challenges the validity of the August 23, 2013 search warrant by claiming the FBI special agent who swore out the federal warrant acted with "a reckless disregard for the truth when he signed the affidavit on which the probable cause finding was based . . ." *Defendant's Brief in Support of Motion to Suppress* (hereafter "*Brief*") at 6. The

defendant argues that he is entitled to an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), during which he would establish the warrant is invalid and that all evidence should be suppressed.

The defendant's motion, however, fails on two separate and independent fronts. First, a review of the search warrant affidavit, in light of applicable law, firmly establishes that the search warrant is sound and that WEED cannot make the required substantial preliminary showing to justify a *Franks* hearing. Second, even if this Court believes that the warrant is somehow vulnerable under a *Franks* analysis, the evidence in this case should not be suppressed because the agents relied in good faith on an extensive search warrant issued by a United States Magistrate Judge.

A. The Search Warrant is Valid and the Defendant Has Not Made a Substantial Preliminary Showing That Would Require a *Franks* Hearing.

As recognized by the Supreme Court in *Franks v. Delaware*, 438 U.S. 154, 171 (1978), there is "a presumption of validity with respect to the affidavit supporting the search warrant." In order to overcome that presumption and mandate an evidentiary hearing to challenge the validity of the warrant, WEED must make a *"substantial preliminary showing"* that:

A. The *affiant* made a knowing and intentional false statement (a "deliberate falsehood"), or included a statement made with reckless disregard for the truth in the affidavit. Allegations of negligence or innocent mistake are insufficient; *and*

B. The allegedly intentional or reckless false statement must be necessary to the finding of probable cause. In other words, if "when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required."

Id. at 155-56, 171-72. Overall, the defendant's burden in establishing the need for a *Franks* hearing, based on either false statements or material omissions, is a "heavy one." *United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994) (citing *Franks*, 438 U.S. at 171-72). The showing

must be more than conclusory and requires a "detailed offer of proof," *United States v. Colkey*, 899 F.2d 297, 300 (4th Cir. 1990), and "allegations of negligence or innocent mistake are insufficient." *Franks*, 438 U.S. at 171; *see also United States v. McKenzie-Gude*, 671 F.3d 452, 462 (4th Cir. 2011) ("Warrant affidavits carry a 'presumption of validity,' and allegations of 'negligence or innocent mistake' provide an 'insufficient' basis for a hearing."). Further, with respect to alleged omissions from an affidavit, the defendant must make a heightened showing that the omissions were "*designed to mislead*, or that are made in *reckless disregard of whether they would mislead*, the magistrate." *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990) (emphasis added).

1. Weed's claim fails under the first Franks prong because he cannot establish that the affiant acted knowingly and intentionally, or with a reckless disregard for the truth.

The key focus for the *Franks* inquiry is on whether the *affiant* acted intentionally or with reckless disregard in providing *false* information in the affidavit. Mere negligence or innocent mistakes are not enough. Rather, the test focuses on "the perspective of the *affiant*" – the defendant must show that the FBI special agent swearing to the affidavit acted "knowingly and intentionally, or with reckless disregard for the truth" in including *false* information in the affidavit. *United States v. White*, 850 F.3d 667, 674 (4th Cir. 2017). The required showing "must be more than conclusory and must be accompanied by a detailed offer of proof." *Colkley*, 899 F.2d at 300 (citation and internal quotation marks omitted).

On this front, WEED claims a *Franks* hearing is warranted because the FBI special agent "had, at minimum, a reckless disregard for the truth" when he included these alleged "false" facts in the affidavit:

1. The affidavit erroneously claims that Comcast IP address **71.61.115.229** is connected to the defendant. WEED counters that the IP address cited in the

FBI report – **71.32.115.229** – is actually connected to a customer of Qwest/Century Link that is located in Albuquerque, New Mexico.[3] He further alleges that the cited address is somehow connected to the FBI through a subunit known as the Biometric Center for Excellence. (*Brief* at 3.)

2. The affidavit fails to note that much of the file data transfers referenced therein actually involved "data transfer[s] **not from** the NRO address, but rather was **to** the NRO address." *Id.* at 3-4 (emphasis in original).

3. The affidavit fails to note that the NRO computer associated with IP address **192.168.55.2** could not store or process any classified information whatsoever, thereby undercutting any probable cause that classified information would have somehow been removed and located at WEED's residence. *Id.* at 4.

Before turning to each of these points in turn, an overarching consideration is the care the *affiant* took in gathering the information is warranted. The FBI special agent, who had 15 years of investigative experience at the time, prepared a *27-page* affidavit in support of probable cause. He reasonably gathered information from NRO investigators and took additional steps to corroborate the information in the warrant. Overall, the affidavit illustrates the affiant's good faith and belies WEED's claims that the agent intentionally provided false information or acted with reckless disregard in providing the information to the magistrate judge. With that background in mind, a review of each category proffered by WEED's counsel shows that the defense cannot clear the first *Franks* hurdle.

a. WEED's Claim that the affidavit erroneously claims that Comcast IP address 71.61.115.229 is connected to the defendant.

WEED claims that the affidavit falsely ties the IP address at the heart of the Remote Desktop Protocol (RDP) sessions (correctly listed in the affidavit as **71.61.115.229**) to his home address. In support, the defendant refers to the IP address cited in FBI Special Agent Jeremy

[3] As explained in greater detail below, the underlined digits are very important. The IP address referenced in the affidavit was correct and was tied to WEED's home address in the manner explained in the affidavit. The IP address referenced by WEED in his motion is incorrect due to a typographical mistake in the FBI report. The undersigned has notified defense counsel of that error.

D'Errico's report – **71.32.115.229**. He also asserts that when he conducted his own internet search on the origins for that address, it comes back as connected to Qwest/Century Link customer located in Albuquerque, New Mexico. (*Brief* at 3.)

The problem for the defendant, however, is that Agent D'Errico's report had a typographical error and should have listed the IP address as **71.61.115.229 –** the same address listed in the affidavit that was actually connected to each of the RDP sessions detailed in paragraphs 16-19 of the search warrant affidavit. Further, as detailed in the affidavit, the affiant issued grand jury subpoenas to Comcast for corroborating details on that specific address. Comcast, in turn, ultimately confirmed that: (1) **71.61.115.229** was one of the company's IP addresses; (2) John WEED had been an active Comcast customer since 2011 with his listed address as the targeted search warrant location; (3) although Comcast no longer had IP address assignment records dating back to the RDP sessions at issue, **71.61.115.229** had been exclusively assigned to WEED's residence during 2013; and (4) that although the 2012 assignment records were no longer available, the same IP address would have likely been exclusively assigned to WEED's residence prior to January 2013.

In sum, WEED cannot begin to establish that the affiant acted recklessly or provided false information on this front. Rather, the above details illustrate the level of work and care exercised by the affiant in pulling together the information presented to the United States Magistrate Judge for his probable cause determination. A *Franks* hearing is not warranted.

b. WEED's claim that the affidavit fails to report that much of the transferred data at the heart of the RDP sessions was actually transferred to the NRO IP address from the outside.

WEED next turns to the RDP sessions referenced in paragraphs 16-19 of the affidavit. As relayed by the affiant in those paragraphs, the FBI Special Agent received details about those

sessions from NRO forensic investigators who conducted a forensic review of the data underlying each of those covert transactions involving WEED. The affiant agent relied on those investigators in good faith and had no reason to question the information they provided. The NRO investigators also provided significant corroborating details for each RDP session as detailed in the affidavit:

- That on September 17, 2012, a government background investigator was attempting to interview WEED about an unreported Driving Under the Influence (DUI) conviction from March 2012. WEED cancelled an interview scheduled for September 18, 2012 and did not sit down with the investigator until September 20, 2012. *Affidavit*, ¶¶ 9-10. During the intervening time, WEED was coming into NRO at unusual hours to execute the RDP sessions at issue. *Id.* at ¶¶ 16(a) and (d), 17(c), 18(c), and 19(c). Further, as relayed in the affidavit, the September 17, 2012 access date coincided with the time-period that the investigator first attempted to interview WEED about the unreported DUI. *Id.* at 16(a).

- The NRO internal computer at the heart of each transfer (later identified by the IP address **192.168.55.2** that is referenced in Special Agent D'Errico's FBI FD-302 report) was located in a Sensitive Compartmented Information Facility (SCIF) within the NRO. Aside from WEED, only seven other individuals had access to that secure room. NRO badge records showed that WEED was the only one out of that group who was present in the building at the time of the transfers. Those same badge records showed the defendant entering the building and the SCIF in the early morning hours (around 5:45 A.M. EST each day) immediately before each RDP session was initiated. *Id.* at ¶¶ 16(d), 17(c), 18(c), and 19(c).

- Each of the RDP transfers were made to a computer named "SUNBLOCK FitPC2." "SUNBLOCK" is a unique name used by WEED to identify himself and the defendant used that display name on all of his NRO related e-mail accounts. *Id.* at ¶¶ 13, 16(a), 17(a), 18 (a), and 19(a).

- Each RDP session from the NRO SCIF was routed to IP address **71.61.115.229**, which was connected to WEED and his residence as described in the previous section and carefully outlined in the affidavit. *Id.* at ¶¶ 17(a), 18(a), 19(a), and 21-22.

- NRO and TASC officials were reasonably concerned that WEED was mentally unstable at the time of the RDP transfers. During a meeting with the government background investigator on September 20, 2012, WEED provided a photo of the officer who arrested him with DUI with bullet holes in it. The defendant explained that he had pulled the picture off the Internet and used it for target practice. He also described how he intended to "ruin the life" of the arresting officer for what he did to the defendant. *Id.* at ¶ 10.

- Interviews of WEED's coworkers revealed the defendant's attitude and desire to "to leave the U.S., if things work out I will never set foot in the US again I will go build toys for someone else" (text sent to CW1) and sell products in Dubai (statement to CW2). *Id.* at 15(a) and (b). The defendant told another coworker (CW3) that he believed the technology he had developed for the NRO was his own intellectual property and that he intentionally would not document his work to prevent it from being reproduced by others. *Id.* at 15(c). WEED also told CW3 words to the effect of "If they ever try to get rid of me I could plant back doors to gain remote access to bring down the systems." *Id.* CW3 and others also knew that the defendant worked from home on NRO projects and likely connected to NRO systems using RDP or File Transfer Protocol (FTP) measures. *Id.*

In addition to the above information, the affidavit included details about the amount of information that WEED was believed to be removing from the NRO during the RDP sessions. The defendant is correct that a subsequent FBI forensic review conducted *one year later* in August 2014 revealed that the majority of data was actually being transferred into the NRO from the IP address connected to the defendant:

RDP Session (Search Warrant Affidavit Paragraphs)	**Reported in August 23, 2013 Search Warrant Affidavit**	**Correct Information Uncovered by FBI Forensic Review Conducted on August 27, 2014**
September 17, 2012 (Affidavit ¶ 16)	133 megabytes (MB) of data transferred out of NRO.	*Data Transferred Out of NRO:* 18.2 MB *Data Transferred In to NRO:* 116.1 MB
September 18, 2012 (Affidavit ¶ 17)	180 MB of data transferred out of NRO.	*Data Transferred Out of NRO:* 15.6 MB *Data Transferred In to NRO:* 167.6 MB
September 19, 2012 (Affidavit ¶ 18)	232 MB of data transferred out of NRO.	*Data Transferred Out of NRO:* 14.9 MB *Data Transferred In to NRO:* 222.7 MB
September 20, 2012 (Affidavit ¶ 19)	279 MB of data transferred out of NRO.	*Data Transferred Out of NRO:* 17.8 MB *Data Transferred In to NRO:* 267.4 MB

Although the NRO investigator who initially interpreted the Wireshark data interpreted that data incorrectly, the defendant falls well short of the *Franks* hearing threshold for two reasons. First, the affiant, FBI Special Agent Steve Hall, reasonably relied on information provided by an NRO forensic investigator back in August 2013 in preparing his affidavit, and reported the exfiltration data, along with substantial corroborating details, in that affidavit.

Contrary to WEED's argument, the affiant's conduct does not begin to approach reckless disregard. It shows, rather, an innocent mistake made by another investigator that was not discovered until one year later. Second, even with the revised figures, the affidavit still established the fact that WEED had established RDP sessions between his computer workstation in an NRO SCIF and his home computer *that were unauthorized*, and that over 66 megabytes of data flowed from the NRO to his IP address during those sessions. Per the metric outlined in the affidavit, one megabyte is the equivalent of 500 double-spaced pages (*Affidavit*, ¶ 16(c)), meaning that WEED removed the equivalent of 33,000 double-spaced pages during his covert RDP sessions at the heart of the affidavit.[4] These realities still establish that the defendant's unauthorized use to a government computer, and at least suggested that government property in the form of digital data was being removed from the NRO. *See id.* at ¶ 20 ("the data transferred on the above dates exceeded any authorized access to the computer system and involved theft of government property").

In sum, the affiant acted in complete good faith in presenting the information outlined in his affidavit. He had no reason to question the exfiltration figures provided by NRO forensic investigators back in August 2013 and did not act in any manner approaching reckless disregard. WEED's argument fails on this front.

[4] The defendant's claim that this removed data is only "acknowledgement packets" (Defendant's Brief in Support of Motion to Suppress, p. 4), falls flat for two reasons. First, the sheer amount of information removed – 33,000 double-spaced pages – flies in the face of any argument that this data was solely acknowledgment packets. Second, the defendant encrypted and compressed the data, and it cannot be unlocked without the proper encryption key. Unless the defendant's expert somehow gets access to that key (which the government does not have), the exact contents of the 33,000 double-spaced pages will remain a question. What is certain, however, is that the defendant exfiltrated government property using a computer within an NRO SCIF.

c. WEED's claim that the affidavit fails to note that the NRO computer associated with IP address 192.168.55.2 could not store or process any classified information.

In his final point of contention, WEED claims that the NRO computer at issue could not store, process, or forward classified information. This fact alone, he claims, shows that the search warrant affidavit is "completely falsified." (*Brief* at 4.) As with his other arguments, this one also falls flat for a number of reasons.

From the outset, the search warrant affidavit provided extensive information about WEED's computer skills and his role as the lead architect for a system that would allow data to flow between classified and unclassified networks. The defendant created the Tactical Dissemination Network (TDN) – a system that was used to process and disseminate information for the military and Intelligence Community in their worldwide anti-terrorism efforts. *Affidavit*, ¶ 8. The TDN was part of the government network that "enables data to flow from unclassified computer systems to classified computer systems, and vice versa." *Id.* at ¶ 20. In addition, "as the designer of this communications platform, WEED potentially had access to" data at varying levels of classification. *Id.* at ¶ 8. These realities, along with the fact that WEED orchestrated the unauthorized RDP sessions from an NRO SCIF, fully illustrate the affiant's good faith and probable cause for the search.

Putting aside, however, that the defendant *could* have removed classified information, the affidavit actually acknowledges that the data removed from the NRO computer may not have been classified. As relayed by the affiant to the United States Magistrate Judge:

> It is *unknown if the data that was transferred consisted of classified or unclassified information***.** However, the nature of the Double Standards letter described above in paragraph 11 suggests that WEED had access to classified information when he wrote the letter. Further, *regardless of the classification*

> *letter, the data transferred on the above dates exceeded any authorized access to the computer systems and involved the theft of government property.*[5]

Affidavit, ¶ 20 (emphasis added). This excerpt also highlights the very point that WEED misses in making his argument – the search warrant is also directed at the defendant's probable violation of criminal statutes that do not hinge on classification issues – 18 U.S.C. § 641 (theft of government property) and 18 U.S.C. § 1030(a)(2) (unauthorized access or exceeding authorized access to obtain information from a protected computer).

Taken together, all of this information (along with other details in the affidavit) highlights the defendant's level of skills and access and completely undercuts his attempt to undermine the probable cause foundation presented to the United States Magistrate Judge. It also, yet again, demonstrates the affiant's good faith in presenting corroborated information within the affidavit, while also acknowledging that he could not say that the transferred data consisted of classified or unclassified information. *Id.* Accordingly, the defendant's request for an evidentiary hearing should be denied in its entirety.

2. Weed cannot satisfy the second Franks prong where the affidavit has ample remaining content supporting probable cause.

As highlighted through the above analysis, WEEDs claims about the IP address connection to his house and the NRO computer's inability to handle classified information are incorrect and the affiant correctly represented information on both fronts. There is also no question that *some amount* of government data was transferred from the NRO to the defendant's residence. The only factual issue remaining is the affiant's inaccurate assertions, of which he

[5] As highlighted in this passage and explained in the affidavit, WEED drafted a letter dated December 24, 2012 (after he had been removed from the NRO and had no access to classified information) that included Secret//SCI level details, names, and locations. The level of detail he provided called into question his ability to pull that classified information from memory, which raised the additional question of whether WEED had continued access to classified information at the time he wrote the letter. *Affidavit*, ¶ 11.

was completely unaware, regarding the *volume of data* that was transferred from WEED's home back to the NRO. To succeed on this front, WEED must show that the including the actual breakdown of incoming and outgoing data during the RDP sessions would defeat probable cause. *See Colkley*, 899 F.2d at 301 (To succeed the defendant must also show that the omitted material was "'necessary to the finding of probable cause,'" *i.e.*, that the omitted material was such "that its inclusion in the affidavit would defeat probable cause,") (quoting *Franks*, 438 U.S. at 156). Even accounting for that additional information, a strong foundation of probable cause still existed for this warrant.

As noted above, the affidavit includes extensive corroborating details about the probable criminal nature of the defendant's RDP session on September 17-20, 2012. Those details included: 1) the background explaining WEED's suspected motive for removing the data prior to his interview with the background investigator; 2) his apparent declining mental state at the same time, as shown by his threats against the arresting officer; 3) records establishing his entry in the SCIF prior to each of the RDP sessions; 4) the fact that the seven other personnel with access to the same SCIF were not present at the time of the RDP sessions; 5) the IP address connection that ties all of the transfers to the defendant's residence; 6) each of the transfers was made to a computer named "SUNBLOCK FitPC2," which includes part of WEED's unique nickname that he gave himself; and 7) interviews of his coworkers illustrating his desire to sell his "toys" to others and that he believed he owned the technology that he had developed for NRO.

These details provide abundant probable cause by themselves, and the volume of data exfiltrated from the NRO is ultimately unnecessary. If one excises from the affidavit the incorrect information regarding the data exfiltrations, the removed language would only address the number of megabytes that were presumably exfiltrated. *But in every RDP session, there was*

an unauthorized outflow of data from the NRO. When properly interpreted, forensic information shows that over 66 megabytes of data, the nature of which remains unknown to this day, was removed from the NRO during the RDP sessions.

For the reasons discussed at length above, this establishes probable cause regarding the defendant's authorized access to a government computer and that he stole government property.[6] *See also Affidavit*, ¶ 20 ("the data transferred on the above dates exceeded any authorized access to the computer system and involved theft of government property"). Thus, even if WEED somehow manages to make it to the second prong of the *Franks* analysis, the probable cause foundation remains sound. His motion fails on this ground as well.

B. Suppression is Not an Appropriate Remedy Because Agents Relied in Good Faith on the Search Warrant Issued by a United States Magistrate Judge.

Even if this Court disagrees with the above arguments made by the Government regarding the finding of probable cause, the evidence in this case should not be suppressed because the agents relied in good faith on an extensive search warrant issued by a United States Magistrate Judge.

The Supreme Court established the rule of good faith reliance on search warrants as an exception to the exclusionary rule in *United States v. Leon*, 468 U.S. 897 (1984). In that case, the Court held that "the marginal or nonexistent benefits produced by suppressing evidence

[6] The same is true even if this Court entertains WEED's argument that removing classified information during these sessions was not possible. In *United States v. Shorter*, 328 F.3d 167 (4th Cir. 2003), the defendant moved to suppress evidence seized during the search of his home, arguing that the affiant had had willfully omitted that he had been told the defendant did not have any marijuana in his apartment at the time of the application. The Fourth Circuit panel rejected the defendant's claim under the second *Franks* prong and reasoned "[e]ven if, as Shorter contends, there could be no probable cause to believe that marijuana would be found in his apartment in light of the omitted fact, the affidavit would still provide ample probable cause to support the issuance of a search warrant for paraphernalia used in marijuana distribution and other indicia of marijuana trafficking." *Id.* at 171. The same reasoning applies here where the warrant sought evidence of criminal violations that turn on theft of government property and exceeding authorized access, as opposed to classification issues.

obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." *Id*. at 922. "Usually, a warrant issued by a magistrate suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotation marks and alteration omitted). However, an officer's reliance on a warrant is not objectively reasonable if:

1) the magistrate or judge was misled by information in an affidavit that the affiant knew was false or would have known was false but for his reckless disregard of the truth;

2) the magistrate wholly abandoned the role of a detached and neutral decision maker;

3) the affidavit supporting the warrant is so lacking in indicia of probable cause as to render the officer's belief in its existence totally unreasonable; or

4) the warrant is so facially deficient, by failing to particularize the place to be searched or the things to be seized, that the executing officers cannot reasonably presume it to be valid.

Id. at 467-70.

WEED's arguments center on the first prong, claiming that the United States Magistrate Judge was misled by information the affiant knew was false, or should have known was false but for his reckless disregard for the truth. For the reasons outlined in the previous section, *supra*, WEED cannot establish that the affiant acted deliberately or with reckless disregard in preparing and presenting the affidavit. At most, the swearing agent made an innocent mistake that was not uncovered until one year later. Further, the search warrant affidavit is very detailed and contains multiple corroborating avenues in support of the magistrate's probable cause determination. Under these circumstances, it was entirely reasonable for the federal agents to rely on this lengthy and thorough search warrant signed by a United States Magistrate Judge. WEED's motion should fail on the good faith front as well.

III. CONCLUSION

For the foregoing reasons, the Court should deny the defendant's motion to suppress.

Respectfully submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

By: */s/ Brian R. Hood*
Assistant United States Attorney
United States Attorney's Office
919 East Main Street, Suite 1900
Richmond, VA 23219
Telephone: (804) 819-5400
Email: brian.hood@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on **September 14, 2018**, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all parties of record.

Respectfully submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

By: */s/ Brian R. Hood*

Assistant United States Attorney
United States Attorney's Office
919 East Main Street, Suite 1900
Richmond, VA 23219
Telephone: (804) 819-5400
Email: brian.hood@usdoj.gov